UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

THE CHILDREN'S PLACE, INC. Plaintiff, v. GREAT AMERICAN INSURANCE COMPANY, Defendant.	:	Case No. 2:18-cv-11963-ES-JAD

DEFENDANT'S BRIEF IN OPPOSITION TO PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF ITS CROSS-MOTION

Ezra H. Alter
ECKERT SEAMANS CHERIN & MELLOTT, LLC
Gateway IV, Suite 401
100 Mulberry St.
Newark, NJ 07102
P: (973) 855-4719
F: (973) 855-4701
ealter@eckertseamans.com

Michael A. Graziano (*pro hac vice*)
ECKERT SEAMANS CHERIN & MELLOTT, LLC
1717 Pennsylvania Ave., NW, Suite 1200
Washington, D.C. 20006
P: (202) 659-6671
F: (202) 659-6699
mgraziano@eckertseamans.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules and Regulations

Additional Authorities

PRELIMINARY STATEMENT

The Children's Place, Inc. ("TCP") seeks to recover under a crime protection policy issued by Great American Insurance Company ("Great American") for two wire transfers TCP made in the aggregate amount of $967,714.29. TCP intended to pay a legitimate vendor, Universal Apparel Co., Ltd. ("Universal"), but an unknown person fraudulently induced TCP employees to transfer the funds to the wrong account by posing as Universal employees in emails. TCP admits the unknown actor did not gain unauthorized access to TCP's computers or email accounts.

TCP cannot recover under the policy, and the Court should enter summary judgment in favor of Great American, for two reasons. First, TCP did not sustain a loss because it did not return the goods that Universal provided in exchange for the payments, and TCP did not issue new payments to Universal. In other words, TCP is currently in the same position it would have occupied if the fraud never occurred.

Critically, TCP cannot claim it will sustain a loss in the future. As TCP itself explained when Universal demanded payment, TCP's contractual liability was discharged when it made payments in good faith even though Universal did not receive the funds. Under well-established principles of contract and agency law, the risk of loss resulting from fraud is borne by the party who was in a better position to prevent the fraud. It is indisputable that Universal was in a better position than TCP to prevent the fraud at issue in this case because the perpetrator obtained the

information that was critical to the success of the scheme by hacking into Universal's email accounts, and because Universal ignored a crucial red flag.

Second, the email scheme upon which TCP's claim is based did not trigger coverage under the policy. TCP paid a separate premium to add an endorsement to the policy which covers losses resulting directly from email-based fraudulent inducement schemes under certain circumstances. As TCP readily admits, however, it failed to comply with a condition precedent to coverage under that endorsement. In fact, the Court has already held that TCP cannot recover under the endorsement.

In light of TCP's admitted failure to satisfy the condition precedent to coverage for email-based fraudulent inducement losses, TCP seeks to recover under two different insuring agreements that were not designed for, and do not cover, such losses. Specifically, TCP seeks coverage under the policy's "computer fraud" and "forgery or alteration" insuring agreements. Neither provision applies.

TCP cites a handful of cases that analyzed email scams under computer fraud insuring agreements. Unlike the policy at issue in this case, however, none of the cases TCP cites involved policies that required a perpetrator to gain "direct access" to the insured's computer system in order for coverage to apply. The "direct access" requirement was added to the industry-standard policy form at issue for the specific purpose of resolving a split in authority by clarifying that ordinary email scams do not trigger computer fraud coverage. The only case that has analyzed the "direct

access" requirement, which TCP conveniently ignores, held that the mere receipt of an email from an imposter is not covered. *Sanderina, LLC v. Great Am. Ins. Co.*, No. 218CV00772JADDJA, 2019 WL 4307854, at *3 (D. Nev. Sept. 11, 2019).

As explained in Section II, the email scheme at issue does not satisfy several additional requirements for coverage under the computer fraud insuring agreement. Furthermore, it is subject to an exclusion which applies to losses resulting from TCP's failure to follow security procedures it represented it would follow. Specifically, TCP represented in its insurance application that it calls vendors at predetermined phone numbers to verify requests to change banking information. TCP admits, however, that it did not follow that procedure with respect to Universal.

TCP's claim for coverage under the forgery or alteration insuring agreement also fails. As the Court held when it previously dismissed that claim, the two documents TCP claims were forged are not the types of financial instruments that are covered by the insuring agreement. The Court granted leave for TCP to amend its complaint based on TCP's vague allegations that different documents may qualify as covered instruments. The only additional documents TCP has identified, however, are emails which fail to satisfy several of the requirements for coverage.

Finally, TCP also seeks to recover fees it allegedly paid to the consultant who determined that TCP's computers were not accessed by any unauthorized users. As explained in Section III, those fees are not recoverable for several reasons.

ARGUMENT

I. TCP HAS NOT SUSTAINED A LOSS OF ANY TYPE.

The most fundamental requirement of each insuring agreement in the policy is that TCP must have sustained a "loss." (J. Statement at ¶¶ 5 & 8; Policy, J. Ex. 1 at §§ B.2 & B.5.)[1] The U.S. Court of Appeal for the Fifth Circuit has succinctly explained the concept of "loss" for purposes of fidelity and crime insurance as follows: "a loss would only result from some action which reduced the available assets in the hands of the [insured] as against its liabilities[.]" *Fid. & Deposit Co. of Md. v. Usaform Hail Pool, Inc.*, 463 F.2d 4, 6 (5th Cir. 1972). In other words, to recover under the policy, TCP must prove that it is in a worse financial position than it would have been if the email scheme had never happened.

TCP has not sustained a loss because it is in the exact same financial position today that it would have occupied if the email scheme never occurred. The joint statement of material facts clearly demonstrates that the total value of TCP's assets has not been diminished. The two payments TCP made are offset by goods TCP admits it actually received from Universal and then re-sold to its own customers, and TCP admits that it has not issued new payments to Universal for those goods:

---

[1] The joint statement of material facts does not cite exhibits by number because the parties had not yet assigned joint exhibit numbers when they filed the statement. For the Court's convenience, this brief cites both the joint statement and the joint exhibit numbers where appropriate.

> 95. All of the amounts TCP transferred to the Thief's account correspond to legitimate payment obligations TCP owed to Universal for goods that Universal had provided to TCP. . . .
>
> 96. TCP did not return the goods to Universal and instead sold them to TCP's customers. . . .
>
> 97. TCP has never issued new payments to Universal for the goods. . . .

(J. Statement at ¶¶ 95-97; [redacted] Dep., J. Ex. 17 at 53:15-54:13, 55:18-57:7, 56:7-12, 57:8-11.)

Since TCP's payments were offset by the goods it received, the only way TCP could sustain a loss as a result of the scheme is if the payments did not discharge its contractual obligation to pay for the goods such that TCP may at some point in the future be held liable and ordered to issue new payments to Universal. Despite the fact that nearly three years have passed, however, "Universal has not filed a lawsuit, served a demand for arbitration, or commenced any other type of legal proceeding against TCP."[2] (J. Statement at ¶ 100; [redacted] Dep., J. Ex. 17 at 60:4-7.)

In any event, Universal would not prevail against TCP if it did sue. As TCP itself stated in an October 14, 2017 email in response to a demand from Universal,

---

[2] The Great American policy does not provide liability insurance, and it does not grant any rights or benefits to Universal. (J. Statement at ¶¶ 20-21; Policy, J. Ex. 1 at § C.17.) Condition 17 explicitly states that the policy "is for [TCP's] benefit only. It provides no rights or benefits to any other person or organization." (*Id.*)

"'as a result of the compromise of [Universal's] email system, [TCP] made good faith payments on the invoices in question' and, therefore, 'no additional amounts are due and owing on these invoices.'" (J. Statement at ¶ 98 (quoting 10/14/2017 Email, J. Ex. 13); *see also* [redacted] Dep., J. Ex. 17 at 62:23-64:17.)

Significantly, TCP's corporate designee under Rule 30(b)(6) of the Federal Rules of Civil Procedure, Peter Khun, testified that the October 14, 2017 email accurately stated TCP's then-current position:

> Q. Is this e-mail an accurate reflection of TCP's position?
> A. Yes.
> Q. Has TCP changed its position since October 14, 2017?
> A. No.

([redacted] Dep., J. Ex. 17 at 64:12-17.)

TCP's Vice President, Assistant General Counsel, [redacted], was copied on the email and was present during the deposition of TCP's corporate designee. (*Id*. at 61:14-23; 10/14/2017 Email, J. Ex. 13.) [redacted] did not, on either occasion, contradict the statement that TCP is not liable to Universal because the misdirected payments were the result of Universal's email system being hacked.

TCP's outside counsel made an unfounded speaking objection to suggest to the witness that a straight-forward question about TCP's position was somehow misleading, and even offered to testify himself when he was apparently displeased with the witness' testimony. ([redacted] Dep., J. Ex. 13 at 62:23-64:11.) At no point,

however, did TCP's corporate designee, its in-house counsel, or its outside counsel indicate that TCP had reversed course and taken the position that it is contractually liable to issue new payments to Universal. (*See id*.)

After discovery closed and the Court ordered the parties to file statements of fact in support of their requests for leave to move for summary judgment, TCP changed its position and submitted its own separate statement which asserts that "TCP had a legitimate payment obligation to Universal that remains open. . . ." (TCP Statement at ¶ 2.) The only evidence TCP cites in support of that statement is [redacted] testimony. (*Id*. (citing [redacted] Dep., J. Ex. 17 at 56:13-16, 57:8-58:7).)

The specific testimony TCP cites does not address whether its obligation to pay Universal remained open after the payments at issue. (*See id*.) Accordingly, it does not contradict [redacted] subsequent testimony that the obligation does not remain open. (J. Statement at ¶ 98 (quoting 10/14/2017 Email, J. Ex. 13); [redacted] Dep., J. Ex. 17 at 62:23-64:17.) TCP's statement that it is still obligated to pay Universal, therefore, is not even arguably supported by the evidence TCP cites.

In addition to failing to cite evidence, TCP has not explained the legal basis for its new position that it must pay Universal. That omission is not surprising because TCP's prior position was correct. TCP is not liable for Universal's losses.

Several courts have addressed how the risk of loss should be allocated between innocent parties who are victims of an email-based fraud scheme such as

the one at issue in this case. The courts analyzed the issue under universal principles of contract and agency law, relying primarily on the Uniform Commercial Code, the Restatement (Second) of Contracts, and the Restatement (Third) of Agency. All of those principles led to the same common-sense rule: the risk of loss is borne by the party who was in the best position to prevent the fraud. *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*, 759 Fed. App'x 348, 353-59 (6th Cir. 2018); *Bile v. RREMC, LLC*, No. 3:15cv051, 2016 WL 4487864, at *7-13 (E.D. Va. Aug. 24, 2016); *Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc.*, No. 8:14-CV-2052-T-30TGW, 2015 WL 4936272, at *5 (M.D. Fla. Aug. 18, 2015).

Great American recognizes that weighing the relative fault of two parties is ordinarily a question of fact to be resolved at trial. Under the circumstances, however, no reasonable factfinder could conclude that TCP bears the risk of loss. It is indisputable that Universal was in a better position than TCP to prevent the loss.

Universal and TCP share blame equally for not confirming that the emails they relied upon were sent from accounts using legitimate domain names, and for not picking up the phone to confirm the information in those emails. The only significant distinguishing factors between TCP's conduct and Universal's conduct, however, weigh heavily in favor of placing the blame on Universal.

Courts have considered two key factors in analyzing which party shares more of the blame for failing to prevent an email-based fraud scheme: (1) whether one of

the parties "was negligent in maintaining its email accounts"; and (2) whether one of the parties "knew about 'red flags' alerting it to fraud and failed to notify the other party to the transaction." Katherine Musbach & Reina Dorvilier, *Apportioning the Loss: A Liability and Recovery Analysis for Email-Based Claims*, XXV Fid. L. J. at 65 (Nov. 2019) (analyzing *Beau Townsend*, *Bile*, and *Arrow Truck Sales*). In this case, both factors clearly support placing the risk of loss on Universal.

First, the unknown actor obtained the information that was critical to the success of the fraud scheme by hacking into Universal's email system. (J. Statement at ¶¶ 26-27 (citing [redacted] Dep., J. Ex. 17 at 31:20-32:2, 42:15-25.) The joint statement of material facts is crystal clear on that point:

> 26. The Thief intercepted emails sent between Universal and TCP by hacking into Universal's email system and accessing the email accounts of Universal's employees. . . .
>
> 27. The information that the Thief obtained by accessing the email accounts of Universal's employees was critical to the success of the fraud scheme. . . .

(*Id.*)

By contrast, and as explained in detail in Section II.A.1 below, TCP's own consultant performed a comprehensive forensic examination of TCP's computer systems and emails accounts and confirmed that TCP's systems had not been accessed by any unauthorized users. (J. Statement at ¶¶ 102-122.) Thus, the blame for failing to protect the confidential information that was critical to implementing

the fraud scheme falls exclusively on Universal. If Universal adequately protected its email accounts from unauthorized intruders, the loss would not have occurred.

Significantly, the fact that Universal's email system was hacked is the precise reason TCP itself gave—with the apparent approval of its in-house attorney who was copied on the email—in explaining why it was not obligated to issue new payments to Universal. (*Id*. at ¶ 98 (quoting 10/14/2017 Email, J. Ex. 13); *see also* [redacted] Dep., J. Ex. 17 at 62:23-64:17.) TCP was correct then, and it has not provided any explanation for suddenly changing its position after discovery closed in this case.

Second, Universal's ignorance of a critical red flag was also a necessary factor in causing the loss. The document TCP claims it relied upon in changing Universal's banking information is a [redacted]. (J. Statement at ¶¶ 47-50.) According to TCP, the unknown actor fraudulently induced Universal employees to complete and sign the form by impersonating TCP employees via email. (*Id*.) TCP claims the unknown actor then altered the completed form by adding fraudulent bank account information before sending it to TCP. (*Id*.)

Universal should have known something was amiss when it received the email asking it to complete a [redacted] because the email contains a statement that Universal must have known was false. Specifically, the email indicated that TCP was requesting a [redacted] because Universal had asked TCP to update its bank account information:

> This is Eunice, TCP Vendor Administrator. Nice to work with you.
>
> According to our finance team info, vendor Universal is requesting bank account info update. Please send update and signed vendor setup form our record, and we will send update our NJ team for info update. Thank you.

(6/20/2017 Email, J. Ex. 10 at TCP000252.)

Universal knew it had not, in fact, requested a change in its bank account information because that request was actually made by the unknown actor. (*See* J. Statement at ¶¶ 39-42.) Accordingly, the false statement that Universal had requested the change was a glaring red flag that should have prompted Universal to investigate the authenticity of the email and inform TCP that it had not asked to change its banking information. Instead, Universal completed the form, thereby enabling the unknown actor to complete the fraud scheme. (*Id*. at ¶¶ 49-50.)

Since TCP's good faith payments discharged TCP's contractual obligation to pay for the goods it received from Universal, the Court should hold that TCP did not sustain any loss and enter summary judgment in favor of Great American. At a minimum, however, the Court should deny TCP's motion for summary judgment. Assuming, *arguendo*, the Court finds that the material issue of whether TCP or Universal should bear the risk of loss is genuinely in dispute, then that dispute must be resolved by the factfinder at trial.

II. THE OCCURRENCE AT ISSUE DID NOT TRIGGER COVERAGE.

The Court should deny TCP's motion and enter summary judgment in favor of Great American for a second reason: the email scheme is not covered by the policy under which TCP has sued. TCP seeks coverage under the policy's "computer fraud" and "forgery or alteration" insuring agreements. Neither provision applies.

A. TCP Cannot Recover Under the "Computer Fraud" Provision.

TCP cannot recover under the "computer fraud" insuring agreement because (1) the "computer fraud" insuring agreement does not apply to ordinary email-based fraud schemes that do not involve a third party gaining unauthorized access to TCP's computer systems or email accounts, and (2) the exclusion titled "Failure to Follow Security Procedures" applies as a result of TCP's failure to perform a callback verification before changing the bank account it used to pay Universal.

1. "Computer Fraud" Coverage Is Not Triggered.

The "computer fraud" insuring agreement provides as follows:

> We will pay for loss resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money, securities or other property from your premises or banking premises to a person, entity, place or account outside of your control.

(J. Statement at ¶ 5; Policy, J. Ex. 1 at § B.5.)

The email scheme at issue did not trigger coverage for the simple reason that the unknown actor did not "gain direct access" to a computer system that belonged to TCP or TCP's financial institution. (*Id*.; *see* J. Statement at ¶¶ 102-122.) Instead, the unknown actor sent emails which, from a technical standpoint, were no different than any email sent from anybody in the world to anybody else in the world in the ordinary course of business. (*See* J. Statement at ¶¶ 102-122.)

The facts related to the email scheme are not in dispute. TCP retained a consultant, [redacted] of Mandiant, to perform "a thorough and comprehensive forensic examination of TCP's computer systems and email accounts." (J. Statement at ¶¶ 102-104; [redacted] Dep., J. Ex. 16 at 5:25-6:7, 23:22-31:15, 45:20-25.) [redacted] did not find any evidence that a third party "hacked, logged into, or otherwise gained unauthorized access to any of TCP's computer systems or email accounts." (J. Statement at ¶ 105; Mandiant Report, J. Ex. 14; *see also* [redacted] Dep., J. Ex. 16 at 21:8-23:6, 37:20-38:5; [redacted] Dep., J. Ex. 17 at 45:13-46:17.) To remove any possible doubt, [redacted] confirmed, and TCP explicitly admits, that, "from a technical standpoint, TCP's receipt of the emails was "'no different than any email that's sent by anybody around the world.'" (J. Statement at ¶ 122; [redacted] Dep., J. Ex. 16 at 37:25-38:5.)

TCP asserts that, "'when interpreting an insurance policy, courts should give the policy's words their plain, ordinary meaning.'" (Pl.'s Br. at 5 (quoting *Nav–Its*,

Inc. v. Selective Ins. Co. of Am., 183 N.J. 110, 869 A.2d 929, 933 (2005) (internal quotation marks and citation omitted)).) The plain and ordinary meaning of the phrase "to gain direct access to your computer system[,]" however, does not apply to the act of sending an email. As such, TCP's receipt of emails which were "'no different than any email that's sent by anybody around the world'" did not trigger coverage. (J. Statement at ¶ 122; [redacted] Dep., J. Ex. 16 at 37:25-38:5.)

Nevertheless, TCP argues that merely pressing the send button on an email grants the sender "direct access" to every computer system that receives the email. (*See* Pl.'s Br. at 9-11.) TCP's argument is ridiculous. For example, TCP's interpretation would mean that anybody in the world can gain "direct access" to this Court's computers by simply sending emails to addresses registered with the domain name "njd.uscourt.gov." Obviously, the phrase "direct access" is not used in that manner in common parlance.

TCP does not—and cannot—cite a single case in support of its interpretation of the phrase "direct access." In fact, the only court that has addressed the issue unequivocally rejected TCP's interpretation. *Sanderina, LLC v. Great Am. Ins. Co.*, No. 218CV00772JADDJA, 2019 WL 4307854 (D. Nev. Sept. 11, 2019).

The insured in *Sanderina* sought coverage for an email impersonation scheme similar to the one at issue in this case under a *verbatim* "computer fraud" insuring agreement. *Id*. at *1-2. As in this case, the insured's consultant did not find evidence

that an unauthorized user had accessed the insured's computers or email accounts. *Id*. The court held that coverage was not triggered because "th[e] record d[id] not support a finding that merely sending an email to [the insured's] employee constituted direct access to [the insured's] computer system." *Id*. at *3.

Lacking case law or common sense reasoning in support of its position, TCP cites dictionary definitions for the proposition that the term "access" means to "enter" or "communicate with'" a person or thing. (Pl.'s Br. at 10-11.) According to TCP, sending an email constitutes gaining "direct access" to the recipient's computer because the email "enter[s]" and "communicate[s] with" that computer. (*Id*.)

TCP's argument is specious. Individual terms in an insurance policy "are properly considered in the context that they appear, when viewed against the policy as a whole, and courts should be wary of interpretations that render other policy terms meaningless." *Formosa Plastics Corp., U.S.A. v. Ace Am. Ins. Co.*, No. CIV. 06-5055, 2010 WL 4687835, at *6 (D.N.J. Nov. 9, 2010) (citing *Hardy ex rel. Dowdell v. Abdul–Matin*, 198 N.J. 95, 104 (2009)). As TCP itself asserts, "'a court must consider the insurance contract as a whole, including any endorsements.'" (Pl.'s Br. at 5 (quoting *Prather v. Am. Motorist Ins. Co.*, 2 N.J. 496, 502-03 (1949).)

As with every term in the policy, the term "access" must be considered in the context in which it is used, *i.e.*, as describing the nature of an interaction with a "computer system." TCP does not cite any dictionaries or other secondary sources

which use the term "access" in the context of describing an interaction with a computer system. The Court should not distort the plain and ordinary meaning of the phrase "to gain direct access to your computer system" by applying a generic definition of the word "access" that has nothing to do with computers.

TCP also relies on a revised version of [redacted] report which states that the emails at issue "'accessed'" TCP's computer systems. (TCP's Br. at 11 (quoting J. Statement at ¶ 119; Revised [redacted] Report, J. Ex. 15).) [redacted] testified that the emails at issue "did not result in any third party gaining access to an internal computer system belonging to TCP." (J. Statement at ¶ 112; [redacted] Dep., J. Ex. 16 at 37:20-24 (emphasis added).) He opined, however, that merely sending an email in the ordinary course of business constitutes authorized access to the recipient's external, publicly-accessible email account. (J. Statement at ¶¶ 121 & 122; [redacted] Dep., J. Ex. 17 at 33:24-34:18, 36:7-20, 37:20-38:5 (emphasis added).)

TCP's reliance on [redacted] revised report is misplaced for three reasons. First, opinion testimony is not admissible to aid in the interpretation of unambiguous policy language. *Howard Berger Co., LLC v. Liberty Mut. Fire Ins.*, No. 114CV06592NLHAMD, 2017 WL 2256960, at *4 (D.N.J. May 23, 2017) (citing *Boddy v. Cigna Prop. & Cas. Companies*, 760 A.2d 823, 828 (N.J. App. Div. 2000) (internal citations omitted)). Since neither party contends that the policy is ambiguous, the Court should not rely on [redacted] testimony to interpret the policy.

Second, as noted, TCP itself argues that the Court "'should give the policy's words their plain, ordinary meaning.'" (Pl.'s Br. at 5 (quoting *Nav–Its, Inc*, 869 A.2d at 933 (internal quotation marks and citation omitted)).) Accordingly, it would be inappropriate for the Court to adopt an expert's highly technical definition that does not "comport[] with the literal meaning of the policy language." *Howard Berger Co., LLC*, 2017 WL 2256960, at *4.

Third, and perhaps most importantly, the circumstances surrounding the revised report prove that even [redacted] himself does not use the term "access" to refer to the mere sending of an email. [redacted] did not change his "opinion" until TCP's attorneys asked him to revise his report during the course of this case.

[redacted] initial report describes the emails as "malicious" and states that [redacted] found no evidence of "malicious access" to TCP's email accounts:

> Mandiant's analysis of firewall logs, exported mailboxes, and mail forwarding rules did not identify any evidence of malicious access to the TCP environment.
>
> Mandiant identified malicious emails from the following domain:
>
> - design-unlversal.com

(J. Statement at ¶ 108; [redacted] Report, J. Ex. 14 at GAIC-TCP CLAIM 000817.) If the emails were "malicious" and there was no "malicious access" to TCP's email accounts, as [redacted] stated, then the mere sending of a "malicious" email must not constitute "access" to the receiving account. (*See id*.)

On May 23, 2019—nearly two years after the initial report was issued and long after TCP commenced this action—[redacted] revised the foregoing language by replacing the word "access" with "interaction." (J. Statement at ¶ 117; *compare* [redacted] Report, J. Ex. 14 at GAIC-TCP CLAIM 000817 *with* Revised [redacted] Report, J. Ex. 15 at TCP000219.) During his deposition, [redacted] claimed that he could not recall why he made the change:

> Q. So, the second change is between these two sentences, except the word "access" was changed to "interaction"; correct?
> A. Yes.
> Q. Why did you do that?
> A. I don't recall at this point. I have to imagine it was also to clarify that point. But between "access" and "interaction," I don't recall the reason for that change.

([redacted] Dep., J. Ex. 16 at 38:6-14.)

The difference between the words "access" and "interaction" must not be significant to [redacted] since he does not even remember why he switched them. What is clear, however, is that the issue was important to TCP's attorneys because [redacted] testified that the only reason he revised his report at all was because he "learned it sounded as if the conclusions in the report were perhaps being misunderstood or misinterpreted[.]" (*Id*. at 32:4-9.) When Great American asked an open-ended question about how [redacted] learned his report may have been misinterpreted, TCP's counsel immediately asserted the attorney-client privilege,

and [redacted] confirmed it was "likely counsel" who told him. (*Id*. at 53:16-54:13.) In fact, TCP's former attorney who served the revised report on Great American stated in his cover email that the revisions were based on discussions that TCP's counsel initiated with [redacted] after learning of Great American's position.

Based on the initial report, it is clear that, before TCP's counsel contacted [redacted] to ask him to revise his report, his opinion was that the emails at issue did not "access" TCP's emails or computer systems. (J. Statement at ¶ 108; [redacted] Report, J. Ex. 14 at GAIC-TCP CLAIM 000817.) The Court should not base its interpretation of the word "access" on the fact that [redacted] reversed his opinion to conform to what TCP wanted it to be.

Even if the Court finds that the phrase "direct access to your computer system" could, when considered in a vacuum, refer to the mere act of sending an email, the Court still must consider that phrase "in the context that [it] appear[s], when viewed against the policy as a whole, and . . . be wary of interpretations that render other policy terms meaningless." *Formosa Plastics Corp., U.S.A. v. Ace Am. Ins. Co.*, No. CIV. 06-5055, 2010 WL 4687835, at *6 (D.N.J. Nov. 9, 2010) (citing *Hardy ex rel. Dowdell v. Abdul–Matin*, 198 N.J. 95, 104 (2009)). Analyzing that phrase in conjunction with the other language in the computer fraud insuring agreement makes it clear that coverage applies only when an unauthorized person uses a secure computer system in an unauthorized manner for at least two reasons.

First, interpreting the insuring agreement as applying to every circumstance in which a person "communicates" with a computer in any way would impermissibly render the phrase "direct access" meaningless. The opening phrase of the insuring agreement already states that it covers "the use of any computer[.]" (J. Statement at ¶ 5; Policy, J. Ex. 1 at § B.5.) Standing alone, the phrase "use of any computer" would apply to any circumstance in which a person uses a computer for any purpose, including sending an email. If that was the meaning intended by the parties, as TCP claims, then it would not have been necessary to also state that coverage applies when a third party "gain[s] direct access" to the insured's computer. (*Id*.)

In order for the phrase "direct access" to serve any independent purpose, it must somehow limit the type of computer usage that is covered. (*Id*.) Under TCP's interpretation, however, the terms "use" and "direct access" would be synonymous, rendering the policy's requirement of both redundant.

Second, TCP's interpretation does not make sense in light of the requirement that the method employed by the fraudster to gain direct access to the insured's computer must involve "impersonat[ing]" the insured or its "authorized officer or employee[.]" (*Id*.) Needless to say, it is never necessary to impersonate a company's employee to send an email to the company. As [redacted] explained, anybody can send an email because the systems that receive emails are "publicly accessible." (J. Statement at ¶¶ 12-13; [redacted] Dep., J. Ex. 16 at 36:7-20.)

In fact, the unknown actor did not "impersonate [TCP], or [TCP's] authorized officer[s] or employee[s]" in the emails that supposedly accessed TCP's computers. Instead, the sender impersonated employees of a completely different entity, Universal. (J. Statement ¶¶ 29-45; 6/13/2017 Email String, J. Ex. 5; 6/20/2017 Email String, J. Ex. 10.) For that reason, independent of the "direct access" requirement, the emails that TCP received did not trigger coverage.[3]

To make sense of the "impersonation" requirement, it must be interpreted as limiting coverage to the use of secure computer systems that are ordinarily accessible only by authorized users. In other words, an unauthorized user must impersonate an authorized user to access a secure computer system by, for example, entering the employee's confidential login information into the computer. That interpretation is the only one which gives operative meaning to all of the words in the phrase: "the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution[.]" (*See* J. Statement at ¶ 5; Policy, J. Ex. 1 at § B.5.)

TCP inadvertently illustrates Great American's point by claiming that *Cincinnati Ins. Co. v. Norfolk Truck Ctr., Inc.*, 430 F.Supp.3d 116 (E.D. Va. 2109)

[3] The unknown actor did impersonate TCP employees in the emails it sent to Universal. (J. Statement at ¶ 46.) Since those emails were sent to Universal, and not TCP, however, the sender was not impersonating TCP "to gain direct access to [TCP's] computer system" even under TCP's interpretation of "direct access."

involved "nearly identical factual circumstances and policy language." TCP is correct that the facts at issue in *Norfolk Truck Center* are similar to this case. The policy language is not even close to identical, however, because the policy at issue in *Norfolk Truck Center* did not include the "direct access" or "impersonation" requirements. *Id*. at 124.

The complete text of both insuring agreements is set forth below:

POLICY AT ISSUE IN *NORFOLK TRUCK CENTER*	**THE GREAT AMERICAN POLICY AT ISSUE IN THIS CASE**
We will pay for loss of or damage to "money", "securities" and "other property" resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the "premises" or "banking premises": a. To a person (other than a "messenger") outside those "premises"; or b. To a place outside those "premises".	We will pay for loss resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money, securities or other property from your premises or banking premises to a person, entity, place or account outside of your control.

(*Compare id*. *with* J. Statement at ¶ 5; Policy, J. Ex. 1 at § B.5.)

By arguing that the insuring agreement at issue in *Norfolk Truck Center* is "nearly identical" to the insuring agreement at issue in this case, TCP is necessarily asserting that the following phrase is utterly meaningless: "to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution[.]" (*See id*.) TCP is asking the Court to hold that approximately one third of the words in the insuring agreement

serve no purpose. The Court, however, must interpret the policy in a manner that gives effect to all of its terms. *See, e.g.*, *Formosa Plastics Corp.*, 2010 WL 4687835, at *6 (D.N.J. Nov. 9, 2010) ("courts should be wary of interpretations that render other policy terms meaningless") (citing *Hardy ex rel. Dowdell*, 198 N.J. at 104).

TCP's claim that it intended for the "computer fraud" insuring agreement to apply to ordinary fraudulent inducement schemes is also belied by the fact that TCP paid an additional premium for an endorsement titled "Fraudulently Induced Transfers" that was designed for the specific purpose of adding coverage for fraudulent inducement schemes. (J. Statement at ¶ 11; *see* Policy, J. Ex. 1.) TCP initially sought coverage under the "Fraudulently Induced Transfers" endorsement, but the Court dismissed that claim because TCP did not (and could not) allege that it complied with a condition precedent. (4/5/2019 Op. [D.E. No. 16] at 9-10.)

If the "computer fraud" insuring agreement was broad enough to cover every fraudulent inducement scheme that involves a computer in any way, then TCP's decision to pay an additional premium for an endorsement that provides the same coverage would be inexplicable. TCP's decision to purchase an endorsement it did not need would be especially bizarre considering the fact that the endorsement has a higher deductible and a lower limit of insurance than those applicable to the "computer fraud" insuring agreement. (*See* Policy, J. Ex. 1 at Declarations.) The

most likely explanation is that TCP paid the additional premium because it knew the policy would not cover ordinary fraudulent inducement schemes without it.

Furthermore, the fact that the "fraudulently induced transfer" endorsement exists proves that the parties contemplated the risk of losses associated with fraudulent inducement schemes and knew how to draft language that would clearly provide coverage for such losses. Their decision not to include the same language in the "computer fraud" insuring agreement indicates that they did not intend for it to apply to fraudulent inducement schemes. In fact, the endorsement is based on a standard form that was developed by the Surety and Fidelity Association of America ("SFAA") precisely because courts had correctly held that several versions of the computer fraud insuring agreement were not designed to cover ordinary email-based fraud schemes, but there was a growing demand for such coverage in the marketplace. *See* Michael Davisson, Patricia Michelana Parisi & Lawrence S. DeVos, *Social Engineering Claims*, 23 FID. L. J. 31, 49-52 (2017).

The same issue arose in *Mississippi Silicon Holdings, LLC v. AXIS Ins. Co.*, No. 1:18-CV-231-SA-DAS, 2020 WL 869974 (N.D. Miss. Feb. 21, 2020). The policy at issue in that case included different variations of the insuring agreements at issue in this case, and the insured, like TCP, sought coverage for an email-based fraud scheme. *Id*. at *1-2. The court held that the scheme was not covered under an insuring agreement similar to Great American's "computer fraud" provision

because, amongst other reasons, the policy had a separate insuring agreement that was specifically designed to cover fraudulent inducement schemes, which it referred to by the commonly-used phrase "social engineering." *Id*. at *7.

The court explained its rationale as follows:

> Had the Computer Transfer Fraud provision been intended to cover a loss occurring when a funds transfer was effectuated by an employee acting in good faith reliance upon an electronic instruction which was ultimately determined to be fraudulent (exactly what occurred in this case), the same language used in the Social Engineering Fraud provision could have been incorporated into the Computer Transfer Fraud provision.

Id. at *7. The same logic applies equally to this case.

TCP devotes a significant portion of its brief to discussing a split in authority with respect to the question of whether the causation language in various computer fraud insuring agreements limited coverage to losses involving the unauthorized use of a computer. (Pl.'s Br. at 6-9, 12-16.) TCP overstates the balance of the split in authority, however, by failing to cite several cases which held in favor of the insurer, and by including cases that are factually inapposite.

For example, TCP relies on *Principle Sols. Grp., LLC v. Ironshore Indem., Inc.*, 944 F.3d 886 (11th Cir. 2019). The *Principle Solutions* court did not analyze the type of computer usage that must cause a loss in order for coverage to apply, however, because the insured did not seek to recover under a computer fraud provision. *See id*. at 889. Instead, it sought coverage under an insuring agreement

which applied to "loss resulting directly from a fraudulent instruction directing a financial institution [to transfer funds]." *Id*. at 889. Thus, the insuring agreement at issue in *Principle Solutions* had nothing to do with computer fraud coverage.

TCP's reliance on *Medidata Sols., Inc. v. Fed. Ins. Co.*, 268 F. Supp. 3d 471 (S.D.N.Y. 2017), *aff'd*, 729 F. App'x 117 (2d Cir. 2018), is also misplaced, but for a different reason. While the Second Circuit held that emails sent by a fraudster were the direct cause of the insured's loss, it did so only after finding that the specific emails at issue in that case had """violat[ed] the integrity of the [insured's] computer system" by introducing a malicious "spoofing code" into the computer. 729 F. App'x at 118 (quoting *Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 37 N.E.3d 78, 81 (N.Y. 2015).) Accordingly, the court did not consider whether the mere sending of an email was covered under the policy at issue in *Medidata*.

On the other hand, TCP cites *Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252 (5th Cir. 2016), but conveniently omits several other cases which held that computer fraud insuring agreements did not cover ordinary fraud schemes that involved the use of a computer in some manner but did not involve unauthorized computer usage: *Mississippi Silicon Holdings, LLC*, 2020 WL 869974; *Sanderina, LLC*, 2019 WL 4307854; *Taylor & Lieberman v. Fed. Ins. Co.*, 681 F. App'x 627 (9th Cir. 2017); *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. CV 13-5039-JFW MRWX, 2014 WL 3844627, at *6 (C.D. Cal. July 17, 2014), *aff'd in*

part, vacated in part, 656 F. App'x 332 (9th Cir. 2016); *Kraft Chem. Co., Inc. v. Fed. Ins. Co.*, No. 13 M2 002568, 2016 Ill. Cir. LEXIS 1 (Ill. Cir. Ct. Jan. 5, 2016); *Universal Am. Corp.*, 37 N.E.3d 78; *Great Am. Ins. Co. v. AFS/IBEX Fin. Servs., Inc.*, No. CIV. A. 307-CV-924-O, 2008 WL 2795205 (N.D. Tex. July 21, 2008); *Brightpoint, Inc. v. Zurich Am. Ins. Co.*, No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377, at *7 (S.D. Ind. Mar. 10, 2006).

Each case approached the issue in a slightly different manner. For example, *Apache* focused on the requirement, which is also included in the Great American policy at issue in this case, that a loss must result "directly" from the use of a computer for coverage to apply. Noting that there was "cross-jurisdictional uniformity in declining to extend coverage when the fraudulent transfer was the result of other events and not directly by the computer use[,]" the Fifth Circuit held that an email scheme similar to the one at issue in this case was not covered. *Apache Corp.*, 662 F. App'x at 258.

Brightpoint and *Pestmaster* focused on the separate requirement, which is also included in the Great American policy at issue in this case, that a computer must be used to "fraudulently cause a transfer" of funds. *Pestmaster Servs., Inc.*, 2014 WL 3844627, at *6; *Brightpoint, Inc.*, 2006 WL 693377, at *7. As the *Pestmaster* court noted, that phrase indicates that coverage applies only when an unauthorized user directly initiates a transfer of funds via computer, as opposed to merely transmitting

fraudulent information to dupe an authorized user into voluntarily initiating a transfer. *Id*.; *see also InComm Holdings, Inc. v. Great Am. Ins. Co.*, No. 1:15-CV-2671-WSD, 2017 WL 1021749, at *10 (N.D. Ga. Mar. 16, 2017), *aff'd sub nom. Interactive Commc'ns Int'l, Inc. v. Great Am. Ins. Co.*, 731 F. App'x 929 (11th Cir. 2018) ("The Fifth Circuit also reviewed decisions from other jurisdictions and found that courts repeatedly have denied coverage under similar computer fraud provisions, except in cases of hacking where a computer is used to cause another computer to make an unauthorized, direct transfer of property or money.")

The courts that found in favor of insurers recognized that interpreting a computer fraud insuring agreement as applying to every fraud that involves the use of a computer in any way does not make sense because it would effectively extend coverage to all fraud given the central role computers play in modern commerce. As the Ninth Circuit explained in affirming the relevant holding in *Pestmaster*: "Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a 'General Fraud' Policy." 656 F. App'x at 333; *see also Apache*, 662 F. App'x at 258; *InComm Holdings, Inc.*, 2017 WL 1021749, at *11 ("*Apache*, and the cases it discusses, warn that to find coverage based on the use of a computer, without a specific and immediate

connection to a transfer, would effectively convert a computer fraud provision into a general fraud provision.")

In any event, this Court does not need to decide which line of cases is more persuasive. In response to that split in authority, the SFAA, and Great American by adopting the SFAA's standard form, added a "direct access" requirement to make it clear that the "computer fraud" insuring agreement does not apply to ordinary email-based fraud schemes. As previously explained, the only court that has interpreted the "direct access" requirement held that coverage is not triggered by the mere receipt of an email which contains fraudulent content. *Sanderina, LLC*, 2019 WL 4307854.

Finally, *Apache* warrants additional consideration because it involved a factually indistinguishable claim under a Great American policy and was decided before the policy at issue in this case incepted. Even assuming this Court would have resolved *Apache* differently if it were in the Fifth Circuit's position in 2016, the decision that the Fifth Circuit did make unquestionably evidences Great American's intent when it subsequently issued the policy in this case to TCP in 2017.

Furthermore, TCP had constructive, if not actual, knowledge of Great American's interpretation of its computer fraud insuring agreements because *Apache*, while unpublished, is not an obscure opinion. Indeed, the first page of results from a Google search of the phrase "Great American Computer Fraud

Insurance" includes a blog that TCP's own counsel in this case, Hunton Andrews Kurth LLP, published about the *Apache* decision on October 21, 2016.

The computer fraud insuring agreement at issue in *Apache* was identical to the one at issue in this case except that the former did not include a "direct access" or "impersonation" requirement. (*Compare* J. Statement at ¶ 5; Policy, J. Ex. 1 at § B.5 *with Apache*, 662 F. App'x at 254.) Great American added those requirements to fortify the "computer fraud" insuring agreement against the types of interpretive arguments that were made by the insureds in *Apache* and the other cases cited above.

The plain meaning of the terms in the insuring agreement, the context in which those terms are used, the fact that TCP paid an additional premium for the "fraudulently induced transfers" endorsement, the legal background against which the "direct access" requirement was added to the insuring agreement, the only case which has addressed that requirement, and common sense all lead to the same conclusion: the mere act sending of an email does not trigger coverage under the "computer fraud" insuring agreement even if the email contains fraudulent content. Accordingly, the Court should find that TCP's claim is not covered.

2. The "Failure to Follow Security Procedures" Exclusion Applies.

TCP's claim is also subject to an exclusion to the computer fraud insuring agreement which applies to losses which result from the insured's failure to follow

certain security procedures. (*See* J. Statement at ¶ 6; Policy, J. Ex. 1 at p. 13.) The exclusion provides that Great American will not pay for:

> (1) loss resulting from your failure to follow **security procedures** agreed to in writing with your customer or your financial institution;
>
> (2) loss that would have been avoided if you had accepted and followed commercially reasonable **security procedures** that your financial institution made available for your account or accounts involved in the loss; or
>
> (3) loss resulting from your failure to comply with **security procedures** that you represented to us you would follow.

(*Id*.)

TCP's claim is subject to sub-paragraph (3) of the exclusion because TCP failed to comply with a security procedure that it represented it would follow. Specifically, the application TCP submitted to obtain the "fraudulently induced transfers" endorsement affirmatively represented that TCP would: "'Verify any request to change the vendor's bank account information by calling the vendor at a telephone number previously provided by the vendor.'" (J. Statement at ¶ 15 (quoting Endorsement Application, J. Ex. 3).) TCP readily admits, however, that it "did not verify the request to change Universal's bank account information by calling Universal at a telephone number previously provided by Universal before

making the change[.]" (J. Statement at ¶¶ 88, 93; [redacted] Dep., J. Ex. 17 50:11-53:14.) As a result, the payments TCP made to the fraudulent account are excluded.

TCP has argued that the callback verification procedure it represented it would follow does not qualify as a "security procedure" under the definition set forth in the policy. The definition provides as follows:

> **Security procedure** means a procedure established by agreement of the Insured and its customer or financial institution for the purpose of (i) verifying that a **payment order** is that of the Insured, or (ii) detecting error in the transmission or the content of the **payment order** or communication. A **security procedure** may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices.

(J. Statement at 7; Policy, J. Ex. 1 at § C.1.)

The callback procedure TCP represented it would follow is obviously the type of procedure contemplated by the policy because one of the specific examples listed in the definition is "callback procedures[.]" (*Id*.) Nevertheless, TCP argues that a procedure cannot satisfy the definition if it was not agreed upon by TCP's "customer or financial institution." (*See id*.) According to TCP, the callback procedure it represented it would follow does not satisfy that requirement because it was not agreed upon by a TCP customer or financial institution.

The Court should reject TCP's interpretation because it would improperly render two of the three sub-paragraphs in the exclusion meaningless. *See Formosa*

Plastics Corp., U.S.A., 2010 WL 4687835, at *6 (citing *Hardy ex rel. Dowdell*, 198 N.J. at 104)). Sub-paragraph (1) of the exclusion is broadly-phrased to apply to all security procedures "agreed to in writing with [TCP's] customer or [TCP's] financial institution." (J. Statement at ¶ 6; Policy, J. Ex. 1 at p. 13.) If TCP's interpretation of the definition is correct, then every single procedure that could conceivably meet the definition of "security procedure" would be subject to sub-paragraph (1) of the exclusion. If so, sub-paragraphs (2) and (3) would serve no purpose whatsoever.

The Court should interpret the policy in a manner that gives effect to all of its terms, including sub-paragraph (3) of the "failure to follow security procedures" exclusion. Applying that exclusion as it is written, there can be no question that it applies in this case as a result of TCP's admitted failure to follow a security procedure it represented it would follow when it applied for the policy.

B. The "Forgery or Alteration" Insuring Agreement Does Not Apply.

The only other insuring agreement under which TCP seeks coverage is the "forgery or alteration" provision, which states, in relevant part, as follows:

> We will pay for loss resulting directly from **forgery** or alteration of checks, drafts, promissory notes, or similar written promises, orders, or directions to pay a sum certain in **money** that are:
>
> (1) made or drawn by or drawn upon you;
>
> (2) made or drawn by one acting as your agent; or that purport to have been so made or drawn.

(J. Statement at ¶ 8; Policy, J. Ex. 1 at §B.2.)

TCP cites five documents that it claims give rise to coverage under the "forgery or alteration" insuring agreement. (TCP's Br. at 18-19.) The exhibit numbers and descriptions for those documents as set forth in the parties' joint exhibit list are as follows:

JOINT EXHIBIT NO.	JOINT EXHIBIT DESCRIPTION
5	Email string dated June 13, 2017 through July 17, 2017
6	Letter dated June 13, 2017 on Universal's letterhead
7	Spreadsheet listing outstanding Universal invoices
10	Email string dated June 20, 2017 through June 21, 2017
11	[redacted]

(Pl.'s Br. at 18-19; J. Ex. List.)

The Court has already held that the allegedly forged letter (Joint Exhibit 6) and the allegedly altered [redacted] (Joint Exhibit 11) are not covered because "neither of these documents references 'a sum certain in money.'" (4/25/2019 Op. at 9.) TCP does not argue that the Court should reconsider its decision in that regard. In fact, TCP does not argue that any of the individual documents it relies upon satisfies all of the requirements necessary to qualify as a covered instrument under the "forgery or alteration" insuring agreement.

For example, TCP does not—and cannot—claim that any of the documents the Court has not already addressed were forged or altered. As demonstrated above,

the additional documents TCP relies upon consist of two email strings (Joint Exhibits 5 and 10) and a spreadsheet that was supposedly attached to one of the emails (Joint Exhibit 7). (*See* TCP's Br. at 18-19.) Neither TCP's brief nor the statements of fact submitted by the parties suggest that any of those documents were forged or altered.

The policy defines forgery as "the signing of the name of another person or organization with intent to deceive; it does not mean a signature which consists in whole or in part of one's own name signed with or without authority, in any capacity, for any purpose." (Joint Statement ¶ 9; Policy J. Ex. 1 at § C.7.) The insuring agreement is also subject to a "Facsimile Signatures" condition which provides: "We will treat a reproduction of a handwritten signature the same as handwritten signature. An electronic or digital signature is not treated as a reproduction of a handwritten signature." (J. Statement at ¶ 10; Policy, J. Ex. 1 at p. 19.)

Some of the emails TCP cites contain typed names. Merely typing a name does not necessarily constitute an electronic or digital signature. Even if it did, however, the policy does not treat an electronic or digital signature as a reproduction of a handwritten signature. (*Id.*) Accordingly, it cannot be a "forgery." (*See* Joint Statement ¶ 9; Policy J. Ex. 1 at § C.7.)

Nor do the emails constitute "alterations." TCP has never claimed that the unknown actor took existing emails and somehow altered those emails before sending them to TCP. Instead, it simply claims that the unknown actor posed as

Universal employees by sending emails from accounts that appeared to be, but were not, from legitimate Universal email addresses. (*See* J. Statement at ¶¶ 28-45.)

The only other document TCP cites is the spreadsheet. The spreadsheet, however, does not contain any marks that could even arguably be described as a signature, much less a signature that falls within the policy's definition of "forgery." (Spreadsheet, J. Ex. 7.) Like the emails, TCP has never claimed that the spreadsheet was somehow altered by the unknown actor in a fraudulent manner.

Moreover, the emails and spreadsheet are not covered for the independently-dispositive reason that they are not the types of financial instruments to which the insuring agreement applies. As the Court explained when it dismissed TCP's claim previously, the "forgery or alteration" provision applies only to documents which are "'*similar*' to "'checks, drafts, promissory notes[.]'" (4/25/2019 Op. at 9.) In addition, coverage is limited to documents which are: "(1) made or drawn by or drawn upon you; (2) made or drawn by one acting as your agent; or . . . purport to have been so made or drawn." (J. Statement at ¶ 8; Policy, J. Ex. 1 at §B.2.)

It should go without saying that "emails containing directions to pay money [a]re not similar to checks or drafts." *Sanderina, LLC*, 2019 WL 4307854, at *3 (D. Nev. Sept. 11, 2019); *Taylor & Lieberman*, 681 F. App'x at 628-29; *see also Metro Brokers, Inc. v. Transp. Ins. Co.*, 603 F. App'x 833, 835 (11th Cir. 2015) (holding that electronic fund transfers were not covered). Unlike the documents listed in the

insuring agreement, emails are not financial instruments that permit the holder to demand payment upon presentment. *Sanderina* and *Taylor & Lieberman* are directly on point, and both cases held that emails similar to the ones at issue in this case were not covered instruments under similar insuring agreements. So too should this Court.

Moreover, the emails do not satisfy the separate requirement that, to be covered, a document must be "made or drawn by or drawn upon" TCP or its agent. (J. Statement at ¶ 8; Policy, J. Ex. 1 at §B.2.) "[T]he phrases 'drawn by' and 'drawn upon' are not ambiguous and have a definite legal meaning." *Travelers Cas. & Sur. Co. of Am. v. Baptist Health Sys.*, 313 F.3d 295, 298-99 (5th Cir. 2002). A "maker" is one who makes a promise to pay and a "drawer" is one who orders a payment to be made on his or her behalf by a third party who is holding the funds. *Id.*; *see also* N.J. Stat. Ann. § 12A:3-103(a)(3) & (5). The emails that the unknown actor sent to TCP did not promise or order a payment. Like the invoices at issue in *Baptist Health*, they requested that payments be made to the sender of the emails.

The spreadsheet TCP relies upon also is not similar to checks, drafts, or promissory notes, and it was not made or drawn by, or drawn upon, TCP. (*See* Spreadsheet, J. Ex. 7.) The spreadsheet also is not covered for those reasons.

Having failed to point to a single document that qualifies as a covered instrument, TCP argues that the five documents it cites should be "[v]iewed together[.]" (Pl.'s Br. at 19.) TCP does not, however, cite any case which held that

the type of documents at issue can be viewed as a single financial instrument for purposes of a "forgery or alteration' insuring agreement.[4]

TCP's only explanation for its position is that the documents, when viewed together, are "similar to checks, drafts, and promissory notes" because "they are capable of inducing, and, indeed, did induce, payment of the amounts indicated." (Pl.'s Br. at 19.) Once again, TCP is asking the Court to violate one of the most fundamental rules of construction by interpreting an insuring agreement in a manner that would render most of its terms meaningless.

Every document that has ever been used to commit a fraud of any type was "capable of inducing, and, indeed, did induce, payment of the amounts indicated." (Pl.'s Br. at 19.) If the "forgery or alteration" insuring agreement covers every document that could possibly be used to commit fraud, then most of the language in that agreement is pointless. For example, the requirement that a document be "made or drawn by or drawn upon" TCP or its agent would serve no purpose if every document that is capable of inducing somebody to make a payment is covered. (J. Statement at ¶ 8; Policy, J. Ex. 1 at §B.2.)

[4] TCP made a similar argument in its opposition to Great American's motion to dismiss and, at that time, cited several inapposite cases. Since TCP did not cite those cases in its brief in support of its motion for summary judgment, Great American does not address them in this brief.

III. TCP CANNOT RECOVER MANDIANT'S ALLEGED FEES.

In addition to the two payments for which TCP seeks coverage, TCP seeks to recover $42,200 it claims to have paid to Mandiant. (Pl.'s Br. at 22-24.) TCP argues that Mandiant's fees are recoverable on the grounds that they were a "mitigation expense" and are covered by an endorsement to the policy which allows Mandiant to recover 50% of the "'reasonable expenses incurred by the Insured in establishing the existence and amount'" of a covered loss up to a limit of $100,000. (*Id*. at 24 (quoting Policy, J. Ex. 1 at Endorsement 16).)

TCP cannot recover consequential damages such as Mandiant's fees because TCP did not sustain a covered loss. If a covered loss had occurred, however, TCP still would not be entitled to summary judgment for at least four reasons.

First, pursuant to the Court's orders dated February 18, 2020, and May 20, 2020, "the parties are bound by their respective statements of fact" that were filed on March 3, 2020. (2/18/2020 Order [D.E. 53]; *see also* 5/20/2020 Order [D.E. 65] (ordering the parties to refile the statements "without any alterations[.]").) Neither the joint statement of facts nor the separate statement that TCP filed say anything about the fees TCP claims it paid to Mandiant or references the exhibits TCP now relies upon in connection with the alleged fees. The Court should enforce its orders and hold that TCP is bound by its statements of fact, which are silent as to the fees.

Second, the new exhibits TCP cites do not prove that TCP actually made any payments to Mandiant. TCP cites its own vague answer to an interrogatory, which states only that "Mandiant/FireEye has billed a total of 105.5 hours to the matter for a total of $42,200[.]" (Pl.'s Supp. Answer to Interrog. 15, TCP Ex. 13.) Assuming it is true, however, the fact that Mandiant "billed" $42,200 does not mean TCP paid it. If TCP did pay Mandiant, it would be simple for TCP to produce evidence of that payment. TCP, however, not provided any evidence of payment.

The only other evidence TCP cites are two invoices it claims to have received from Mandiant. (9/12/2017 Invoice, TCP Ex. 1; 4/13/2019 Invoice, TCP Ex. 2.) Obviously, the fact that an invoice exists does not prove it was paid.

Moreover, the invoices raise more questions than they answer because they do not even match the amount stated in TCP's interrogatory answer. (*Compare id*. *with* Pl.'s Supp. Answer to Interrog. 15, TCP Ex. 13.) The total amount of the invoices is $64,500, but TCP's interrogatory answer states that Mandiant billed $42,500. (*Id*.) TCP has not provided any explanation for this inconsistency or any evidence of what amount, if any, it actually paid.

Third, TCP has not established that either of the conflicting amounts in the invoices and interrogatory answer relate to mitigation or investigative expenses in connection with the transactions at issue in this case. The only information provided in the interrogatory answer is that "Mandiant/FireEye has billed a total of 105.5

hours to the matter for a total of $42,200[.]" (Pl.'s Supp. Answer to Interrog. 15, TCP Ex. 13.) In order to analyze whether some or all of the 105.5 hours that Mandiant supposedly billed were spent on mitigation or investigative-related tasks, it is necessary to know what Mandiant did during those 105.5 hours. TCP, however, has never provided those details.

The invoices TCP cites also do not provide any detail about the specific services that were billed. (9/12/2017 Invoice, TCP Ex. 1; 4/13/2019 Invoice, TCP Ex. 2.) Moreover, the second invoice appears to relate to a monthly fee that Mandiant billed for services it was providing nearly two years after the occurrence at issue in this case because the invoice is dated April 13, 2019, and states that the unit of measurement is "Mth." (4/13/2019 Invoice, TCP Ex. 2.) Obviously, any monthly services TCP was receiving from Mandiant in April of 2019 are not reasonably related to mitigating or investigating the specific occurrences at issue in this case.

Great American attempted to obtain more information during a deposition of TCP under Rule 30(b)(6) deposition. Despite the fact that the first topic listed in the notice of deposition was TCP's damages, TCP's corporate designee had no knowledge about TCP's billing arrangement with Mandiant. ([redacted] Dep., J. Ex. 17 at 95:13-96:23) In fact, he admitted that some of the fees included in the $42,200 may relate to services provided in connection with this litigation, such as preparing [redacted] for his deposition:

Q. Okay. And it relates to—well, primarily, Mandiant's fee, which billed a total of 105.5 hours to the matter for a total of 42,200, correct?
A. Correct.
Q. Mandiant charged by the hour, I take it?
A. Presumably. I don't have knowledge of the arrangement with them—
Q. If I—
A. — the billing arrangement.
Q. You don't have knowledge of the billing arrangement, okay. Do you know this 105.5 hours, what it all consists of? I mean, I don't want to ask you, like, granular details, you know, he spent .1 sending an e-mail to someone.

Just, in general, does the 105.5 hours all relate to the initial investigation of the system, or does it also include things that occurred later, for example, like [redacted] deposition?
A. I don't know the full details. I don't know if the deposition is explicitly within the 105 hours, but, presumably, the lion's share of that chunk is the—for the services.
Q. But you're not sure exactly how it's calculated, sitting here today?
A. No.

(*Id.*)

Needless to say, any fees Mandiant billed in connection with [redacted] deposition or in preparing the revised report that TCP's counsel asked [redacted] to prepare for use in this litigation are not recoverable as mitigation or investigative expenses. Since TCP has failed to prove the amount, if any, that Mandiant billed for

services that may be recoverable, the Court should deny TCP's summary judgment with respect to Mandiant's fees.[5]

Fourth, TCP has made no effort to establish that the amount Mandiant billed was reasonable in relation to the services provided, which is an explicit requirement under the cases TCP cites and the policy endorsement under which it seeks to recover. (*See* Pl.'s Br. at 23-24.) Since TCP has not provided any evidence of what Mandiant did during the 105.5 hours it supposedly billed, it is impossible for Great American or the Court to analyze the reasonableness of the amount of time that Mandiant spent and, therefore, the amount of the fees it billed.

CONCLUSION

The Court should enter summary judgment in favor of Great American because TCP did not sustain a loss and the occurrences upon which its claim is based did not trigger coverage under the Great American policy. At a minimum, however, the Court should deny TCP's motion for summary judgment because TCP has not demonstrated the absence of a genuine dispute of material fact with respect to whether TCP is contractually liable to issue new payments to Universal, and, therefore, whether TCP sustained a loss in connection with the transactions at issue.

---

[5] Not only did TCP fail to adequately prepare its Rule 30(b)(6) representative or produce evidence to explain how Mandiant's fees were calculated, TCP refused to provide such evidence in response to a recent request. Great American intends to file a separate letter seeking leave to file a motion for, amongst other things, sanctions based on TCP's failure to comply with its discovery obligations.

DATED: June 8, 2020.

GREAT AMERICAN INSURANCE COMPANY

/s/ Ezra H. Alter
Ezra H. Alter
ECKERT SEAMANS CHERIN & MELLOTT, LLC
Gateway IV, Suite 401
100 Mulberry St.
Newark, NJ 07102
P: (973) 855-4719
F: (973) 855-4701
ealter@eckertseamans.com

Michael A. Graziano (*pro hac vice*)
ECKERT SEAMANS CHERIN & MELLOTT, LLC
1717 Pennsylvania Ave., NW, Suite 1200
Washington, D.C. 20006
P: (202) 659-6671
F: (202) 659-6699
mgraziano@eckertseamans.com

Counsel for defendant

CERTIFICATE OF SERVICE

I hereby certify that, on June 8, 2020, the foregoing was served via email on:

Kevin V. Small, Esq.
HUNTON ANDREWS KURTH LLP
200 Park Avenue
52nd Floor
New York, NY 10166

Walter J. Andrews
Daniel Hentschel
HUNTON ANDREWS KURTH LLP
1111 Brickell Avenue, Suite 2500
Miami, FL 33131
(305) 810-2500

Counsel for plaintiff

/s/ Ezra H. Alter
Ezra H. Alter